International Journal of Trend in Scientific Research and Development (IJTSRD)
Volume 5 Issue 1, November-December 2020 Available Online: www.ijtsrd.com e-ISSN: 2456 – 6470

A Study on Honeypots and Deceiving Attacker using Modern Honeypot Network

Anil Tom[1], Dr. M N Nachappa[2]

[1]Master of Computer Application, [2]Professor,
[1,2]Jain Deemed-to-be University, Bangalore, Karnataka, India

ABSTRACT

A honeypot is a widely used security control to capture and analyse malicious network traffic. The main goal of honeypot is to monitor and receive log data, which can later be used to prevent future attacks. It imitates the contact between emulated computer and attacker with the objective of acquiring sufficient data for effective analysis and potential prevention of attacks. A honeypot is used to detect intruders in many fields such as defence, Government sectors, enterprises, higher institutions, Banking sectors, Nuclear reactors and many more. There are two types of honeypots that are deployed for different uses - research honeypots and production honeypots. Research honeypots are focused on gathering information about the attack, used specifically for the purpose of learning about hacking methodologies. Production honeypots, on the other hand, are focused primarily on diverting attacks from important systems. This work detects the type of the intruders, analyses their strategy and strength of the attack. The deployment of honeypot detects various kinds of attacks using different sensors. Server is deployed in the cloud environment and sensors can be deployed in either in cloud or in Raspberry pi or machine. Server displays the feeds from sensors which is placed over different locations. Live rendering of attacks is shown in the dashboard and honey map points the exact geographic locations using longitude and latitude values. These logs can be further used to analyses and take essential measures in defence perspectives.

Keywords: *Honeypot, Honeynet, Honeymap, Modern Honeypot Network*

How to cite this paper: Anil Tom | Dr. M N Nachappa "A Study on Honeypots and Deceiving Attacker using Modern Honeypot Network" Published in International Journal of Trend in Scientific Research and Development (ijtsrd), ISSN: 2456-6470, Volume-5 | Issue-1, December 2020, pp.266-271, URL: www.ijtsrd.com/papers/ijtsrd35900.pdf

IJTSRD35900

1. INTRODUCTION

With an ever-increasing number of methods and tactics used to attack networks, the goal of securing a network must also continually expand in scope. While traditional methods such as Intrusion Detection System (IDS)/Intrusion Prevention Systems (IPS), Demilitarized zone (DMZ), penetration testing and various other tools can create a very secure network, it is best to assume vulnerabilities will always exist, and sooner or later, they will be exploited. Hence, there is a need to continuously find innovative ways of countering the threats, and one such way is to deploy honeypots on top of standard security mechanisms. If we've ever wondered how the good internet guys are going after the bad guys, one way is something that's called a honeypot. We see, in addition to the security measures we would expect, including securing a computer network to keep cyber criminals out, the good guys use a honeypot to do just the opposite, attract the bad guys.

In computer security terms, a cyber-honeypot works in a similar way, baiting a trap for hackers. It's a sacrificial computer system that is intended to attract cyber- attacks, like a decoy. It mimics a target for hackers, and uses their intrusion attempts to gain information about cybercriminals and the way they are operating or to distract them from other targets. Figure 1.0 shows the overview of a honeypot. A honeypot is a computer or Raspberry Pi intended to mimic likely targets of cyber-attacks.

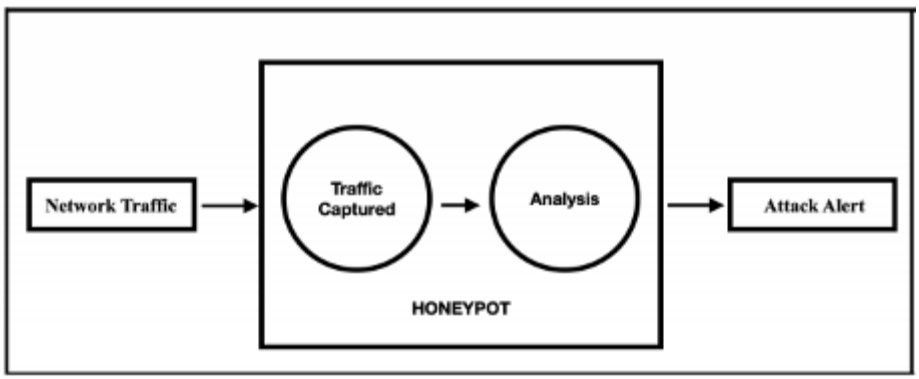

Figure 1.0

It can be used to detect attacks or deflect them from a legitimate target. It can also be used to gain information about how cybercriminals operate. Honeypots mimic an organisation's network environment, which would trick a hacker to assume that it is an actual organisation. For example, a honeypot could mimic a company's customer billing system, a frequent target of attack for criminals who want to find credit card numbers. Once the hackers are in, they can be tracked, and their behaviours assessed for clues on how to make the real network more secure. There are many applications and use cases for honeypots, as they work to divert malicious traffic away from important systems, get an early warning of a current attack before critical systems are hit, and gather information about attackers and their methods.

A honeypot is a widely used security control to capture and analyse malicious network traffic. The main goal of honeypot is to monitor and receive log data, which can later be used to prevent future attacks. It imitates contact between emulated computer and attacker with the objective of acquiring sufficient data for effective analysis and potential prevention of attacks.

2. OBJECTIVES

The Honeypot system is used to detect the type of the intruders, analyse their strategy and strength of attack. There are two categories of honeypots that are deployed for different uses - research honeypots and production honeypots. Research honeypots are focused on gathering information about the attack, used specifically for the purpose of learning about hacking methodologies. For example, the Honeynet Project is a volunteer project that runs honeypots to assess cyber threats. Production honeypots, on the other hand, are focused primarily on diverting attacks from important systems. Information gathering is also very important, since the data can be used to further secure the real production systems, as well as for forensic or legal purposes.

3. TYPES

The honeypots can be classified into two that are

- Based on level of interaction
- Based on purpose

A. Based on level of interaction

Based on the level of interactions between attacker and the system there is three types of honeypots are the that are,

- Low-interaction honeypots
- Medium-interaction honeypots
- High-interaction honeypots

➢ Low-interaction honeypots

In the Low-interaction honeypots, it have only limited interaction with the external system. We can choose FTP as an example for the low-interaction honeypot. They are easy to deploy and maintain, with many security teams deploying multiple honeypots across different segments of their network.

➢ Medium-interaction honeypots

The medium-interaction honeypots are also called as mixed-interactive honeypots. These types of honeypots are more advanced than low-interaction honeypots but less than when we compared to high-interaction honeypots. The medium-interaction honeypots gives intruder with a more advanced illusion of operation system, so that the more advanced attacks can be logged to our system and we can analyse that. They emulate aspects of the application layer, but do not have their own operating system. They work to stall or confuse attackers so that organisation's have more time to figure out how to properly react to an attack.

➢ High-interaction honeypots

The high-interaction honeypots are the most sophisticated types of honeypots. It actually look like a same as the original and which gives the intruder or attacker the realistic experience and so that we can get more advanced logs about the attack and we can analysis it. This type of honeypot allows the deploying organisation to see attacker behaviours and techniques. High-interaction honeypots are resource-intensive and come with maintenance challenges, but the findings can be worth the squeeze.

B. Based on purpose

Based on the purpose we can classify it two,

- Research honeypots
- Production honeypots

➢ Research honeypots

Research honeypots are focused on gathering information about the attack, used specifically for the purpose of learning about hacking methodologies.

➢ Production honeypots

Production honeypots, on the other hand, are focused primarily on diverting attacks from important systems. Information gathering is also very important, since the data can be used to further secure the real production systems, as well as for forensic or legal purposes.

4. DECEIVING ATTACKER USING HONEYPOT

Honeypots are decoy systems or servers deployed alongside production systems within our network. When deployed as enticing targets for attackers, honeypots can add security monitoring opportunities for blue teams and misdirect the adversary from their true target. Honeypots come in a variety of complexities depending on the needs of our organisation and can be a significant line of defence when it comes to flagging attacks early. There are many applications and user cases for honeypots, as they work to divert malicious traffic away from important systems, get an early warning of a current attack before critical systems are hit, and gather information about attackers and their methods. If the honeypots neither contain confidential data nor well-monitored, one can get insight on attacker tools, tactics, and procedures (TTPs) and gather forensic and legal evidence without putting the rest of our network at risk. Figure 4.0 shows the steps in the deployment of a honeypot.

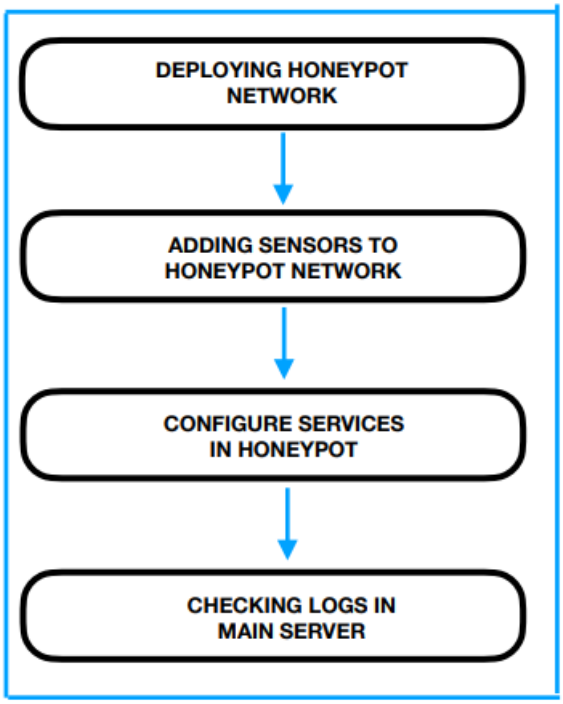

Figure 4.0 Deployment of Honeypot

4.1. COMPONENTS

Honeypot is basically divided into two components: server and sensor. Each component is designed with certain technologies.

A. Server part includes the following:

- **AWS Cloud**

The server part of honeypot is deployed in cloud platform. A web-service is enabled to get a user friendly dashboard, Result or retrieved data from the sensor will be updated over there. Simple UI is designed for the webpage so that output can be easily accessed.

- **Hp Feeds**

It is a light weight authenticated publish-subscribe protocol. It has a simple wire-format so that everyone is able to subscribe to the feeds with their favourite language in almost no time.

- **Mnemosyne**

This technology is used for efficient learning. Flash-card tool in mnemosyne optimizes the learning process. Mnemosyne uses a sophisticated algorithm to schedule the best time for a card to come up for review. Difficult cards that we tend to forget quickly will be scheduled more often, while Mnemosyne won't waste our time on things we remember well.

- **HoneyMap**

HoneyMap is a web application which visualizes a live stream of GPS locations on a SVG world map. In principle, it can be used with any stream of GPS data. Programmers use captures from honeypot, provided by several hpfeeds from the Honeynet

- **Mongo DB**

It is a cross-platform document oriented database program. Classified as a NoSQL database program, it is a document database, which means it stores data in JSON-like documents. Also known as an unstructured database.

B. Sensor part includes the following:

- **Snort**

Snort is open source, lightweight Network IDS for Linux and window to detect threats. Snort can do protocol analysis, content searching/matching, it is also used to detect attacks and probes.

➢ **Dionaea**

It is used to trap malware exploiting vulnerabilities exposed by service offered to networks. The action is to trap or exploit malware that attacks the tissue, and its main purpose is to obtain a copy of the malware.

➢ **Conpot**

It is a low interactive server-side Industrial Control Systems honeypot designed to be easy to deploy, modify and extend. By providing a range of common industrial control protocols. Protocol stacks and templates are created so that Conpot can resemble a real hardware (Uranium centrifuge, Power grid, Aircraft carrier etc.).

➢ **Amun**

Anum is a lightweight and flexible low-interaction honeypot, which is made to capture malware that spreads by exploiting server based vulnerabilities. In our system amun tries to put Drupal (Content Management System) as bait in front of attackers.

4.2. SYSTEM ARCHITECTURE

Honeypot comprises of server and sensor side components. Sensor-side honeypots are a combination of different kinds of honeypots which are deployed for specific tasks. On the other hand, Server-side honeypots deal with the data retrieved by the sensors for output representation. Rather than being a single system, a combination of multiple honeypots deployed in a network is called Honeynet. Figure 4.2 shows the honeypot architecture. In the sensor, honeypot captures all traffic which comes to the environment. Each honeypot captures different kinds of attack for which it is designed. Alert from the sensor will be sent to the server module. Each sensor is embedded with a network scanner and IP tracker.

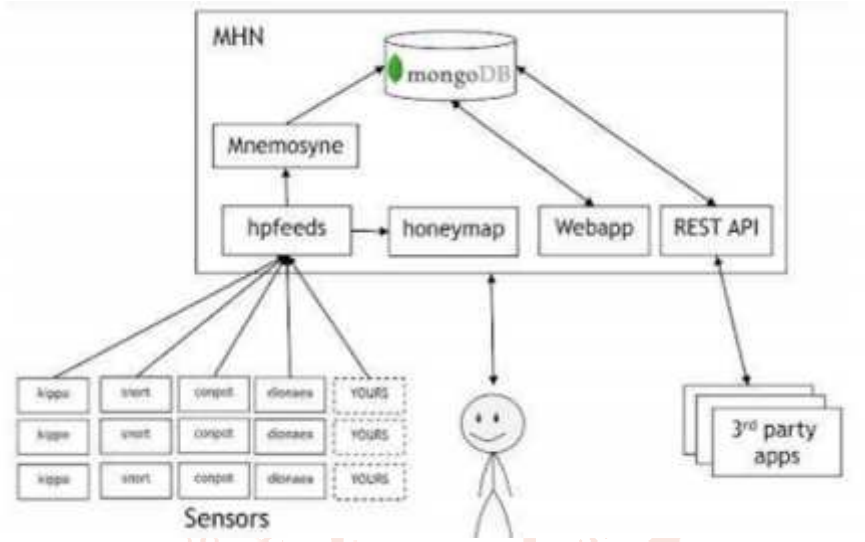

Figure 4.2 Architecture of Honeypot

Sensors are hosts in a system or cloud or Raspberry Pi. Server is hosted in a cloud platform so that it won't be shut down during power failure. Cloud is economic and has a vast storage space. Alert received from the sensor is in the binary format, Hpfeeds converts the binary format into readable language. Output delivered from Hpfeeds will be stored in the Mongo database using a learning tool Mnemosyne. Snort contains certain rules which are considered as parameters to detect malicious content in network traffic. Dashboard or UI provided in the web application which is hosted on the server. Honeymap provide a live streaming off GPS locations.

5. Results and Analysis

Deployed server records all the input provided from the sensors which consist of multiple honeypots. Each sensor captures specific kind of attacks, stored logs and displayed in dashboard which is provided in the web service hosted on the server. The different sensors and the corresponding attack reports are discussed below:

5.1. Dionaea

Dionaea sensor (deployed in cloud) with public DNS (IPv4) 54.209.14.173 captures malware attack from Columbia, Russia, France, USA, Brazil etc. Detailed explanation of source IP, Destination ports, Protocol through the attack mitigated and date and time of attack capture are given in figure 5.1. The countries are represented by their national flags.

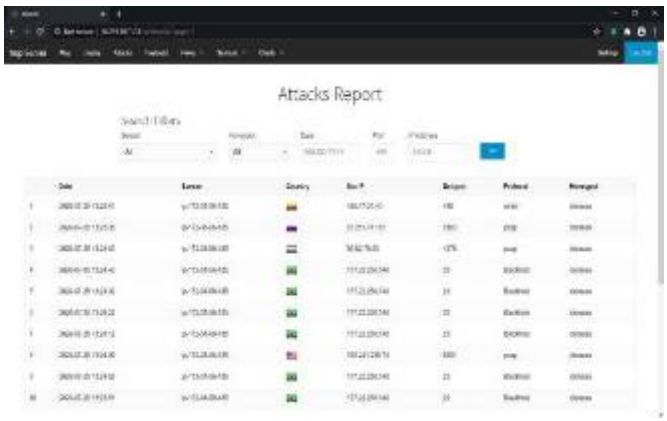

Figure 5.1

5.2. Amun

The attack report of Amun sensor is shown in figure5.2. The attackers targeted the famous ports like 445 (HTTPS), 8080 (HTTP Alternate), 23 (Telnet), 587 (SMTP) and penetrate into Amun sensor using Microsoft-ds, Submission, Telnet, http-alt etc. Sensor has hosted in network IP 172.31.40.145

and it been targeted by Eagle eyes from China, USA, India, Taiwan etc. Content Management System (CMS) and Drupal service is provided in this sensor, which helps to analyse the targeted attacks and tactics.

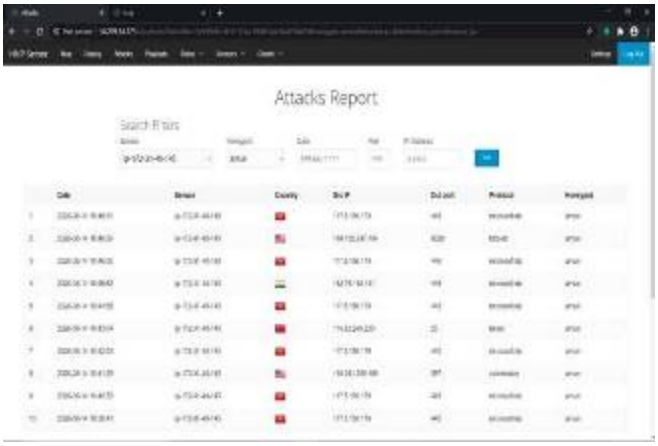

Figure 5.2

5.3. Cowrie

Cowrie is the same as Kippo which is used to capture the brute-force attack and enumerate the strength of it or in other how many combination attackers tried in this attack. Usually this attack targets port 22 (SSH). The figure 5.3 shows the attacks from Macedonia, Russia and France which is captured in common. Figure 5.4 shows the number of combinations of password used in an attempt. The attacker with source IP 85.209.0.100 tries single combinations of password at a time, this shows the strength of brute-force attack is low.

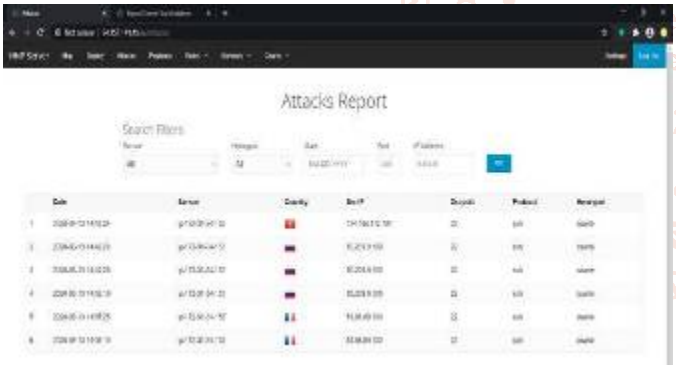

Figure 5.3 Attack report of Cowrie

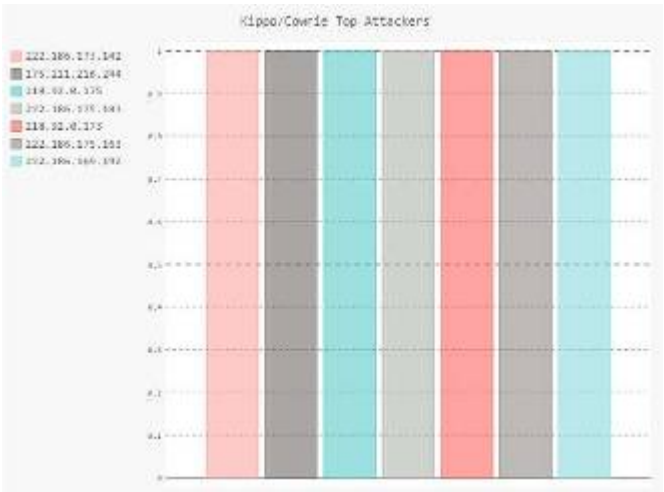

Figure 5.4 Strength of Brute-force attacks in Cowrie

5.4. Snort

Snort is a popular IDS system which helps to block all the malicious traffic. Usually snort consists of certain rules which contain popular malware signatures which helps it to identify the malicious content of traffic. Figure 5.5 depicts the source of attack which is scattered in Russia, China, Germany, France etc. They tried to penetrate through different ports, but they followed the same protocol. Because malicious IPs, signatures and its traffic are blacklisted already, IDS defends and blocks the traffic from those IPs.

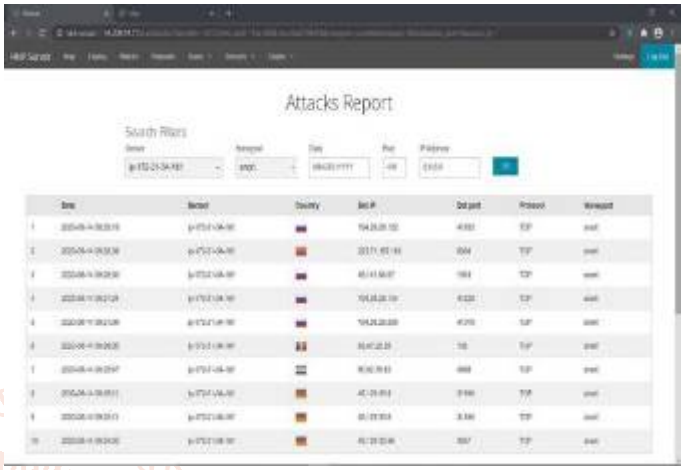

Figure 5.5 Attack report of Snort

Snort rules are a different methodology for performing detection. It is based on detecting the actual vulnerability.

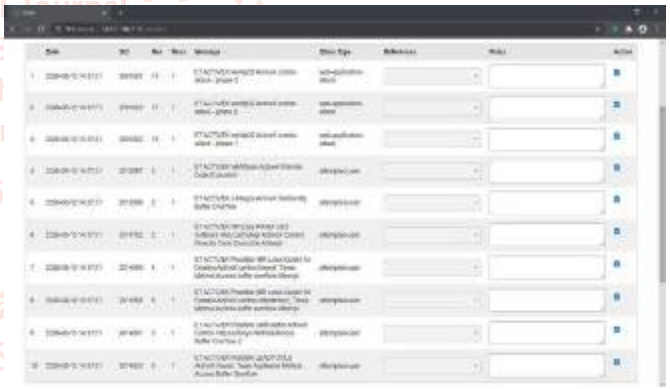

Figure 5.6 Snort Rules

Snort rules are depicted in figure 5.6. The keywords in the figure are explained below:
SID is used to uniquely identify Snort rule
REV is used to uniquely identify revisions of Snort rules
Class Type is used to categorize a rule as detecting an attack that is part of a more general type of attack class
Reference allows the rules to include references to external sources of information

It is considered that snort id is a unique identifier for each rule. It allows output plugins to identify rules easily and should be used with the Rev (revision) keyword.

5.5. Conpot

The Conpot results in figure 5.7 concludes that these kinds of attacks are rare, but strong enough to break into bigger attacks. It captures logs from port 502 (TCP/UDP). The USA is the leading source in this attack where France, Switzerland and Canada hold the corresponding positions.

According to the pattern observed from the report, the source locations are clustered.

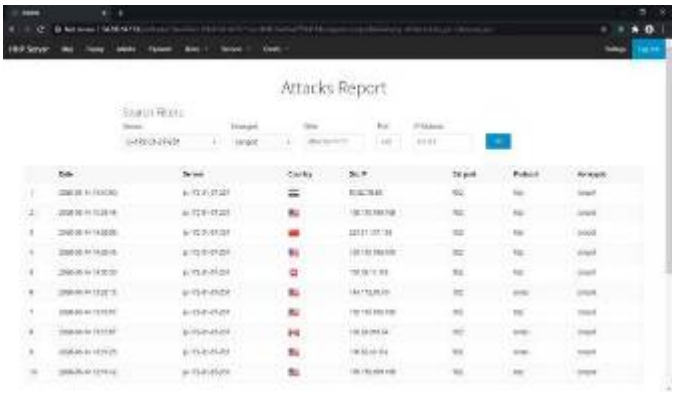

Figure 5.7 Attack report of Conpot

5.6. Honeymaps

Honeymap is a web application which visualizes a live stream of GPS locations on a SVG world map. It can be used with any stream of GPS data which will provide actual latitude and longitude value as it is given in figure 5.8.

Figure 5.8 Honey map

6. CONCLUSION

Once the honeypot management system is implemented, all the honeypots managed to outwit the attackers by opening ports on a server that turned these ports into a hoax are cleared to record the suspicious activities of the attackers. Although the action of intrusion into the system is not optimal, the results are displayed on the web interface which could complement each other in providing information to administrators for further action. Honeypots like Amun, Dionaea, Cowrie, Snort and Conpot are managed to deceive the attackers by opening ports in servers that are often targeted by attackers.

7. FUTURE ENHANCEMENT

Malware analysis can also be embedded into this system. Captured signatures of malware as reference an improved supervised learning can implement in future which can improve the system as well as fasten the entire process.

8. REFERENCES

[1] Haris Semic and Sasa Mrdovic, "IoT honeypot: a multi-component solution for handling manual and Mirai-based attacks", IEEE Open Access Journal, vol.6, November 2017.

[2] Muhammet Baykara and Resul Das, "A novel honeypot-based security approach for real-time intrusion detection and prevention systems", Journal of Information Security and Applications, vol.41, December 2018.

[3] Jicha, Arthur, Mark Patton, and Hsinchun Chen. "SCADA honeypots: An in-depth analysis of Conpot", IEEE conference on intelligence and security informatics (ISI). IEEE, 2016.

[4] M. S. Durairajan, R. Saravanan and S. Sibi Chakkaravarthy, "Low interaction honeypot: a defense against cyber-attacks", Journal of Computational and Theoretical Nanoscience, vol.13, January 2016.

[5] Feng, X., Li, Q., Wang, H., & Sun, L. "Characterizing industrial control system devices on the internet", IEEE 24th International Conference on Network Protocols (ICNP), 2016.

[6] Rushikesh Katkam "Study on Honeypot based secure Network System", International Journal of Advanced Research in Computer Science, vol.10, November 2019.

[7] https://blog.rapid7.com/2016/12/06/

[8] www.honeynet.org/projects/active/conpot/

[9] www.honeynet.org/projects/active/dionaea/

[10] https://www.kaspersky.com/resource-center

[11] www.honeynet.org/projects/active/honeytrap/